configuration so that the device can go into radio resource control (RRC) connected state right away without a need of performing RACH.

[0081] According to a possibility the device gets access to the second, cellular network and is authenticated and authorized for the requested service provided by the machine server and the first network. The second network may facilitate necessary application allowing for the user of the device to confirm to its home network on its willingness and capacity to pay for the requested service. In an embodiment, the cellular network, after authenticating and authorizing the device, configures the device with valid security-access-and-allocation configurations of the machine server and the first network (e.g. new security keys to be applied for the upcoming session between the device and the machine server resource allocation to access machine server), as received from the first network.

[0082] Mobile devices can communicate with the machine type server and the first network over D2M while staying connected to the second, cellular network for possible assistance. The first network and the second network may interact and ask each other to reconfigure or, in general, control and manage the device over either D2M or cellular-access radio interface in a secure and efficient fashion. The second network may get updated of security-access-and-allocation information from the first network and signals that to the device over the cellular air interface when necessary during the service.

[0083] In accordance with an embodiment a mobile device is configured to monitor and report on the D2M link and service quality (including success-failure) to the second network.

[0084] In accordance with an embodiment no sensitive data associated with a mobile device is maintained and permanently stored at a machine server. This feature can be provided to prevent any possible malicious use while e.g. printing from a machine type terminal. This can be realized with e.g. a temporal embedded encryption method applied for the data used by the machine terminal, e.g. when actually printing. Furthermore, upon completing of a service session the first network may send confirmation to the second network and the device that any user data associated with the session is deleted.

[0085] An arrangement of networking functions and procedures to facilitate secure cellular network **2** assisted D2M communications where a machine server **4** provides services for a capable mobile device **5** of the authentic mobile cellular network **2** over a specified D2M air interface **7** will be described below. A device **5** can discover a machine server **4** for possible D2M communications and initiates service request to the machine **4** via the cellular network **2** by calling a unique number assigned to the machine. The discovery may be based e.g. on the user seeing the machine physically and detecting a number assigned to the machine attached physically on the machine or nearby, or discover the identity of the machine over the air, e.g. from a pop-up message shown on the screen of the device. A listing of possible services that the machine can provide may also be displayed. Upon receiving the call request of the device the cellular network **2** can identify the address or number of the machine server **4** and contact network **1** to authenticate and authorize both the machine server and the device for the requested service and service charge. The networks interact and exchange necessary configuration information over the interface **9** there between to enable D2M communications over the specified radio interface **7**.

[0086] In accordance with a possibility network **2** contacted first by the mobile device **5** may request the mobile device **5** to indicate its D2M related capability and software/firmware compatibility information including OS information.

[0087] In accordance with a possibility, the first contacted network **2** activates suitable D2M mode for the mobile device **5** and configures the device with necessary information to get quick access to the machine server **4** and to conduct the requested service. The configuration information may include different security keys and RNTIs to discover and access the machine server.

[0088] In accordance with a possibility, network **1** where the machine server **4** is connected to allocates, and if needed reactivates, the machine server **4** for the requested service. The network **1** may also inform the machine server about the mobile device. This information can include information on assigned RNTIs, software compatibility and/or capability information, and so on.

[0089] In accordance with a possibility, the machine server **4** is configured to advertise at least some system information and some or all access information over the D2M interface **7**. This can be provided in a secure encrypted fashion so as to ensure that only devices which are authenticated and authorized devices are able to acquire up-to-date valid ciphering key from the network **2**. The machine **4** may broadcast information such as its identity, system information, service information, and/or access information to potentials devices.

[0090] Mobile device **5** can use the D2M configuration information received from the cellular network **2** to get access to and requested services in D2M mode. During D2M communications session, the cellular network **2** and the machine network **1** may interact and ask each other to reconfigure or, in general, control and manage the device over either D2M or cellular-access radio interface in a secure and efficient fashion.

[0091] When a D2M connection is provided in a cellular system assisted mode where a connection with the cellular system is maintained for the duration of the service it is possible to recover from a D2M link failure via the regular cellular access. Thus, if the mobile device can be kept in the connected state (DRX or long-sleep dormant) of cellular system until end of the service session. This can also be desired for example when charging takes place is via cellular network billing.

[0092] However, the connected state can also be dropped before the end of the service usage. The length of stay ion connected mode can depend on e.g. service type, capacity to pay and charging option that a user has selected. In the printing example, if a user is able to choose to pay by cash at the M-device site it can be e enough for the cellular network to assist in setting up and/or enabling the use and then drop the connections.

[0093] The mobile device may be kept in RRC connected state with advance Discontinuous Reception (DRX) of the cellular network **2**. This may be advantageous e.g. when other cellular access services are used in parallel. The mobile device can also be moved to RRC idle or long-sleep dormant state but still maintain some active user equipment (UE) contexts in the cellular network.